H-A

#4

03 CO

Attorney's Docket No.: 324-010243-US(PAR)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: LATVA-AHO et al.
Serial No.: 09/827,208
Filed: 4/05/01
For: CONNECTING ACCESS POINTS IN WIRELESS TELECOMMUNICATION SYSTEMS

Group No.:

Examiner:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

TRANSMITTAL OF CERTIFIED COPY

Attached please find the certified copy of the foreign application from which priority is claimed for this case:

Country	**: Finland**
Application Number	**: 20000841**
Filing Date	**: 7 April 2000**

WARNING: "When a document that is required by statute to be certified must be filed, a copy, including a photocopy or facsimile transmission of the certification is not acceptable." 37 CFR 1.4(f) (emphasis added.)

SIGNATURE OF ATTORNEY
Clarence A. Green

Type or print name of attorney

Reg. No.: 24,622

Tel. No.: (203) 259-1800

Perman & Green, LLP

Customer No.: 2512

P.O. Address

425 Post Road, Fairfield, CT 06430

NOTE: The claim to priority need be in no special form and may be made by the attorney or agent if the foreign application is referred to in the oath or declaration as required by § 1.63.

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8a)

I hereby certify that this correspondence is, on the date shown below, being:

☑ MAILING

deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231

Date: 6/11/01

☐ FACSIMILE

transmitted by facsimile to the Patent and Trademark Office

Deborah J Clark
Signature

DEBORAH J. CLARK
(type or print name of person certifying)

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 7.3.2001

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija Applicant	**Nokia Mobile Phones Ltd** **Helsinki**
Patenttihakemus nro Patent application no	**20000841**
Tekemispäivä Filing date	**07.04.2000**
Kansainvälinen luokka International class	**H04M**

Keksinnön nimitys
Title of invention

"Liityntäpisteen liittäminen langattomassa tietoliikenne-järjestelmässä"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

CERTIFIED COPY OF PRIORITY DOCUMENT

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A, P.O.Box 1160, FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

L1

Liityntäpisteen liittäminen langattomassa tietoliikennejärjestelmässä

Keksinnön tausta

Keksintö liittyy liityntäpisteen liittämiseen muihin verkkoelementteihin langattomissa tietoliikennejärjestelmissä.

Matkaviestinoperaattoreiden pääosin omistamien ja kontrolloimien julkisten PLMN-matkaviestinverkkojen (Public Land Mobile Network) lisäksi on kehitetty erilaisia langattomia privaattiverkkoja esimerkiksi yritysten tarpeisiin. Tyypillisesti nämä langattomat privaattiverkot ovat lyhyen kantaman WLAN-verkkoja (Wireless Local Area Network), jotka tarjoavat langattoman yhteyden esimerkiksi toimiston sisällä. Eräitä tärkeitä langattomia lähinnä yksityiskäyttöön tarkoitettuja verkkostandardeja ovat IEEE802.11 WLAN-standardi, TETRA-standardi (Trans-European Trunked Radio) ja DECT-standardi (Digital European Cordless Telecommunications). 3GPP:n (3rd Generation Partnership Project) kehittämä kolmannen sukupolven matkaviestinjärjestelmä UMTS (Universal Mobile Telecommunications System) on järjestelmä, jossa tullaan radiotiellä käyttämään laajakaistaista koodijakomonikäyttöteknologiaa eli WCDMA-teknologiaa (Wideband Code Division Multiple Access). WCDMA-järjestelmässä solun kaikki päätelaitteet käyttävät päätelaitteelta tukiasemalle olevalla siirtotiellä keskenään samaa taajuutta ja taas vastaavasti tukiasemalta päätelaitteelle olevalla siirtotiellä keskenään samaa taajuutta. WCDMA-järjestelmä voidaan matkaviestinjärjestelmien yhteydessä toteuttaa joko taajuusjakokanavointina (FDD-moodi, Frequency Division Duplex) tai aikajakokanavointina (TDD-moodi, Time Division Duplex). TDD-moodia on suunniteltu käytettäväksi erityisesti pienissä pico-soluissa, joita voitaisiin käyttää esimerkiksi kattamaan yrityksen rakennuksien sisäinen langaton viestintä. Tätä tarkoitusta varten voidaan käyttää QPSK-modulaatiota, jolla päästään koodaamattomana päätelaitteen suuntaan (downlink) 5.7 Mbit/s nopeuksiin ja jatkossa 16QAM-modulaatiota (Quadrature Amplitude Modulation), jolla voidaan päästä päätelaitteen suuntaan jopa 11.4 Mbit/s nopeuksiin.

Langattoman tietoliikennejärjestelmän liityntäpisteellä (access point) tarkoitetaan tämän hakemuksen yhteydessä mitä tahansa verkkoelementtiä tai useamman verkkoelementin kokonaisuutta, joka osallistuu langattoman yhteyden tarjoamiseen päätelaitteelle joko suorasti tai epäsuorasti. Liityntäpiste voi olla esimerkiksi tukiasema, yhtä tai useampaa tukiasemaa kontrolloiva radioverkkokontrolleri (tai tukiasemakontrolleri) tai tukiaseman ja radioverkkokont-

rollerin muodostama kokonaisuus. Vaikka tällä hetkellä PLMN-verkkojen, kuten GSM- tai UMTS-verkkojen, liityntäpisteet ovat suurelta osin operaattoreiden hallinnassa, jatkossa myös PLMN-verkkojen liityntäpisteitä voi olla enenevässä määrin myös yksityiskäytössä. Yksityiskäytöllä tarkoitetaan sekä yksittäisten henkilöiden tai organisaatioiden käyttöä. Lisäksi, operaattorit voivat olla halukkaita luovuttamaan liityntäpisteverkon hallintaa muille tahoille esimerkiksi alihankinnaksi. Liityntäpisteiden yhdistäminen muihin tietoliikennejärjestelmän verkkoelementteihin aiheuttaa kuitenkin ongelmia. Muita verkkoelementtejä, kuten runkoverkkoa, hallitsevalla operaattorilla ei ole tehokasta keinoa kontrolloida liityntäpisteiden yhdistämistä muihin verkkoelementteihin. Liityntäpisteen yhdistäminen muihin tietoliikennejärjestelmän osiin vaatii asetusten säätöä, joten liityntäpisteiden siirtäminen tai uusien liityntäpisteiden käyttöönotto ei ole helppoa eikä onnistu kovinkaan nopeasti. Liityntäpisteistä yhteys muihin verkkoelementteihin voi olla järjestetty julkisen verkkojen, kuten Internetin kautta, mikä aiheuttaa turvallisuusriskejä.

Keksinnön lyhyt selostus

Keksinnön tavoitteena on kehittää uudenlainen tapa käyttää liityntäpisteitä. Keksinnön tavoitteet saavutetaan menetelmällä, langattomalla tietoliikennejärjestelmällä ja langattoman tietoliikennejärjestelmän liityntäpisteellä, joille on tunnusomaista se, mitä sanotaan itsenäisissä patenttivaatimuksissa. Keksinnön edulliset suoritusmuodot ovat epäitsenäisten patenttivaatimusten kohteena.

Keksintö perustuu ajatukseen käyttää IC-kortteja (Integrated Circuit) liityntäpisteissä. IC-kortille tallennetaan tietoja liityntäpisteen liittämiseksi toiminnalliseen yhteyteen kiinteän verkko-osan kanssa. Kiinteä verkko-osa voi käsittää yhden tai useampia olennaisesti kiinteitä verkkopalveluita tarjoavia verkkoelementtejä. Kun halutaan liittää liityntäpiste kiinteään verkko-osaan, kytketään IC-kortti toiminnalliseen yhteyteen liityntäpisteen kanssa. Tarvittavia kiinteän verkko-osan resursseja liitetään liityntäpisteen kanssa toiminnalliseen yhteyteen mainittujen tallennettujen tietojen perusteella.

Tästä saavutetaan se etu, että uusia liityntäpisteitä saadaan helpommin liitettyä muihin verkkoelementteihin, koska IC-kortilla on jo ennalta tallennettuna tarvittavia tietoja. Operaattoreille tarjoutuu lisäksi uusi dynaaminen tapa yhdistää asiakkaan vastuulla olevat verkkoresurssit osaksi operaattorin omaa tietoliikenneverkkoa. Operaattori voi antaa liityntäpisteen liittämiseen tarvittavat tiedot käsittävän IC-kortin valitsemalleen taholle. Tämä mahdollistaa

joustavan ja turvallisen tavan käyttää yksityisiä liityntäpisteitä ja tilapäisesti käyttää esimerkiksi vuokrattavia liityntäpisteitä IC-kortin käsittämien tietojen avulla. IC-kortin käyttäminen liityntäpisteissä tarjoaa operaattorille mahdollisuuden luovuttaa liityntäpisteiden hoidon jollekin valitsemallensa taholle tai ostaa liityntäpisteiden tarjoamat palvelut.

Keksinnön erään edullisen suoritusmuodon mukaisesti kiinteässä verkko-osassa tarkastetaan, onko IC-kortilla oikeus käyttää kiinteän verkko-osan resursseja. Tarvittavia kiinteän verkko-osan resursseja liitetään liityntäpisteen kanssa toiminnalliseen yhteyteen, jos IC-kortilla on oikeus käyttää kiinteän verkko-osan resursseja.

Tästä edullisesta suoritusmuodosta saavutetaan se etu, että kiinteän verkko-osan haltija saa helposti ja luotettavasti kontrolloitua, että vain valtuutetuilla tahoilla (joiden IC-kortilla on riittävät oikeudet) on oikeus liittää liityntäpisteensä, esimerkiksi tukiasemansa, muihin verkkoelementteihin.

Vielä keksinnön eräiden edullisten suoritusmuotojen mukaisesti IC-kortti autentikoidaan kiinteässä verkko-osassa ja liityntäpisteen ja kiinteän verkko-osan välinen liikenne salataan IC-kortin käsittämien tietojen perusteella. Tällöin voidaan varmistua IC-kortin aitoudesta ja liityntäpisteen ja kiinteän verkko-osan välinen liikenne voidaan välittää turvallisesti julkisenkin verkon kautta.

Kuvioiden lyhyt selostus

Keksintöä selostetaan nyt lähemmin edullisten suoritusmuotojen yhteydessä, viitaten oheisiin piirroksiin, joista:

Kuvio 1 esittää erästä UMTS-järjestelmää;

Kuvio 2 esittää keksinnön erään edullisen suoritusmuodon mukaista langatonta tietoliikennejärjestelmää;

Kuvio 3 havainnollistaa IC-kortin sisäistä rakennetta pelkistettynä lohkokaaviona;

Kuvio 4 havainnollistaa signalointikaaviona liityntäpisteen liittämistä kiinteään verkko-osaan; ja

Kuvio 5 havainnollistaa erästä tapaa autentikoida IC-kortti.

Keksinnön yksityiskohtainen selostus

Keksintöä voidaan soveltaa missä tahansa liityntäpisteitä käsittävässä langattomassa tietoliikennejärjestelmässä. Seuraavassa keksinnön

erästä edullista suoritusmuotoa kuvataan UMTS-järjestelmässä siihen kuitenkaan rajoittumatta.

Viitaten kuvioon 1 selostetaan esimerkinomaisesti UMTS-järjestelmän rakennetta. UMTS-järjestelmän pääosat ovat runkoverkko (core network) CN, maanpäällinen radioverkko (UMTS Terrestrial Radio Access Network) UTRAN ja matkaviestin tai tilaajapäätelaite (user equipment) UE. CN:n ja UTRAN:in välinen rajapinta on nimeltään Iu, ja UTRAN:in ja UE:n välinen ilmarajapinta on nimeltään Uu.

UTRAN muodostuu tyypillisesti useista radioverkkoalijärjestelmistä (radio network subsystem) RNS, joiden välinen rajapinta on nimeltään Iur (ei kuvattu). RNS muodostuu radioverkkokontrollerista (radio network controller) RNC ja sen ohjauksessa olevasta yhdestä tai useammasta tukiasemasta tai B-solmusta (node B), joita kutsutaan kuviossa 1 esitetyn suoritusmuodon yhteydessä liityntäpisteiksi AP. RNC:n ja liityntäpisteen AP välinen rajapinta on nimeltään Iub. RNC hoitaa Iub-rajapinnan siirtoresurssien varaamisen ja kontrollin. RNC kontrolloi monelta osin liityntäpisteen AP resursseja. RNC välittää tarvittavia järjestelmätietoja (System Information) liityntäpisteelle AP. RNC kontrolloi jaettuja kanavia (Shared Channels) ja yhteisiä kanavia (Common Channels), kuten hakukanavia (Paging Channels). Pääsääntöisesti RNC kontrolloi myös dedikoituja kanavia (Dedicated Channels) ja päättää päätelaitteelle UE varattujen yhteyksien siirroista solujen välillä (handover). Liityntäpiste välittää tarvittaessa erilaisia mittausraportteja esimerkiksi teho- ja häiriötasoista. Iub-rajapinnassa suoritetaan myös liityntäpisteiden AP ja radioverkkokontrollereiden synkronointi.

Tilaajapäätelaite UE voi olla esimerkiksi kiinteästi sijoitettu, ajoneuvoon sijoitettu tai kannettava mukana pidettävä päätelaite. Päätelaite UE käsittää tyypillisesti IC-kortille tallennetun USIM-sovelluksen (UMTS Subscriber Identity Module), jota käytetään erityisesti oikean käyttäjän identifioimiseksi PIN-tunnisteen (Personal Identity Number) avulla, USIM-sovelluksen autentikoimiseksi runkoverkossa CN, käyttäjän (joka voi olla tilaaja) edustamiseksi runkoverkossa CN ja yhteyden salaamiseksi päätelaitteen UE ja liityntäpisteen AP välillä.

On huomattava, että UMTS-järjestelmä on suunniteltu siten, että runkoverkko CN voi perustua esimerkiksi GSM-järjestelmän runkoverkkoon, jolloin koko verkkoinfrastruktuuria ei tarvitse rakentaa uudelleen. GSM-järjestelmään pohjautuva runkoverkko CN muodostuu UTRAN:in ulkopuoli-

sesta matkaviestinjärjestelmään kuuluvusta infrastruktuurista. Piirikytkentäisiä yhteyksiä hoitaa tyypillisesti vierailijarekisterin VLR (Visitor Location Register) käsittävä matkaviestinkeskus 3GMSC/VLR, josta voidaan järjestää yhteydet ulkopuolisiin verkkoihin, kuten yleiseen analogiseen (PSTN, Public Switched Telephone Network) tai digitaaliseen ISDN-verkkoon (Integrated Services Digital Network) tai Internetiin.

Runkoverkkoon CN voi myös kuulua GPRS-tekniikkaan (General Packet Radio Service) pohjautuva pakettiradiojärjestelmä, joka käsittää yhdyskäytäväsolmun GGSN (Gateway GPRS Support Node) ja operointisolmun SGSN (Serving GPRS Support Node). Operointisolmun SGSN tehtävänä on havaita GPRS-yhteyksiin kykenevät päätelaitteet palvelualueellaan, lähettää ja vastaanottaa datapaketteja kyseisiltä päätelaitteilta sekä seurata päätelaitteiden sijaintia palvelualueellaan. Yhdyskäytäväsolmu GGSN toimii yhdyskäytävänä GPRS-verkon ja ulkoisen dataverkon PDN (Packet Data Network) välillä. Ulkoisia dataverkkoja voivat olla esimerkiksi toisen verkko-operaattorin GPRS-verkko, Internet, X.25-verkko tai yksityinen lähiverkko. Yhdyskäytäväsolmu GGSN on yhteydessä kyseisiin dataverkkoihin rajapinnan Gi kautta. Operointisolmu SGSN sekä matkaviestinkeskus 3GMSC/VLR hyödyntävät tilaajatietoja olennaisesti pysyvästi käsittävää kotirekisteriä HLR (Home Location Register). UMTS-järjestelmän tarkemman kuvauksen osalta viitataan 3GPP:n UMTS-spesifikaatioihin.

Kuviossa 2 on esitetty keksinnön erään edullisen suoritusmuodon mukaista UTRAN-radioverkkoa, jossa liityntäpiste AP toimii tukiasemana. Tilaajapäätelaite UE voi kommunikoida liityntäpisteen AP kanssa radiorajapinnan Uu yli. Liityntäpisteeseen AP voidaan syöttää IC-kortti ICC, jolle on tallennettu tietoja, joita voidaan tarvita liityntäpisteen aktivoinnissa ja/tai liityntäpisteen liittämisessä kiinteään verkko-osaan, erityisesti radioverkkokontrolleriin RNC ja edelleen runkoverkkoon CN. Kiinteä verkko-osa on yleinen termi mille tahansa olennaisesti langallisia yhteyksiä tarjoavan verkon yhdelle tai useammalle verkkoelementille; kuviossa 2 kiinteän verkko-osan resurssit käsittävät mm. radioverkkokontrollerin RNC. IC-kortilla ICC tarkoitetaan tyypillisesti luottokortin kokoista muovista korttia, johon on asetettu mikroprosessori ja muistia.

Liityntäpiste AP käsittää lähetinvastaanotinvälineet TXRX, tyypillisesti useita radiorajapinnan (Uu) lähetinvastaanottimia UuTXRX ja korttivälineet ICCM ainakin yhden IC-kortin ICC käyttämiseksi liityntäpisteessä AP. Edelleen liityntäpiste AP käsittää muistia MEM ja loogisen ohjausyksikön

CONTROL, joka ohjaa lähetinvastaanottimien UuTXRX, lähetinvastaanotinvälineiden TXRX ja korttivälineiden ICCM toimintaa muistin MEM avulla. Ohjausyksikkö CONTROL voidaan toteuttaa esimerkiksi prosessorissa suoritettavana ohjelmistona. Lähetinvastaanotinvälineillä TXRX voidaan muodostaa kaksisuuntainen yhteys muihin kiinteän verkko-osan elementteihin, kuten radioverkkokontrolleriin RNC, ja niillä voidaan siirtää useiden lähetinvastaanottimien UuTXRX käyttämät liikenne- ja ohjauskanavat Iub-rajapinnan siirtoyhteydelle. Liityntäpisteen AP radiorajapinnan lähetinvastaanottimista UuTXRX on yhteys antenniyksikköön ANT, jolla toteutetaan kaksisuuntainen radioyhteys päätelaitteeseen UE.

Kuten kuviossa 2 on havainnollistettu, liityntäpiste AP voi olla yhteydessä kiinteään verkko-osaan esimerkiksi Internetin kautta. Jos liityntäpisteen AP ja kiinteän verkko-osan välinen yhteys on järjestetty julkisen verkon yli, IC-kortin ICC käsittämiä tietoja voidaan edullisesti hyödyntää myös siirrettävän datan salaamiseen. Tyypillisesti käytetään myös tulimuureja (Firewall), joita ei ole esitetty kuviossa 2. Yhteys voidaan järjestää muodostamalla IC-kortin ICC käsittämien tietojen perusteella virtuaalinen erillisverkko (VPN, Virtual Private Network), jolloin lähetettävät IP-paketit lähetetään kapseloituna Internetin yli ja näinollen käytettävä yhteys on suojattu. Liityntäpisteen AP ja kiinteän verkko-osan välinen linkkitason yhteys voidaan järjestää esimerkiksi Ethernetiä tai ATM-tekniikkaa käyttäen (Asynchronous Transfer Mode).

Kiinteä verkko-osa käsittää edullisesti liityntäpisterekisteripalvelimen APRS (Access Point Register Server) ja liityntäpistepalvelimen APS (Access Point Server) IC-kortin ICC käytön tukemiseksi. APRS käsittää tyypillisesti IC-kortin myöntäjän muodostaman tietokannan, joka käsittää olennaisesti pysyvästi tietoja liityntäpisteitä varten luovutetuista IC-korteista ICC. APRS käsittää edullisesti tietoja IC-kortin ICC haltijasta, tietoja kortin ICC autentikoimiseksi ja tiedon, onko IC-kortilla ICC oikeus käyttää kiinteän verkko-osan resursseja. Tiedot on edullisesti eroteltu IC-kortille ICC yksilöllisen tunnisteen mukaisesti ja APRS voi edelleen käsittää tarkempaa tietoa IC-kortille ICC sallituista resursseista tai asetuksista. Liityntäpisterekisteripalvelin APRS käsittää myös välineet tietokannassa olevien tietojen käyttämiseksi, tietojen tallentamiseksi, prosessoimiseksi ja käskyjen muodostamiseksi.

Keksinnön erään edullisen suoritusmuodon mukaisesti liityntäpisteeseen AP syötetylle IC-kortille ICC on tallennettu osoitetieto liityntäpisterekisteripalvelimesta APRS. Tällöin haluttaessa liittää liityntäpiste AP kiinteän

verkko-osan resursseihin käyttäen IC-korttia ICC muodostetaan yhteys liityntäpisterekisteripalvelimelle APRS. Liityntäpiste AP voidaan liityntäpisterekisteripalvelimen APRS sen salliessa liittää edullisesti kiinteän verkko-osan radioverkkokontrolleriin RNC APRS:n valitseman liityntäpistepalvelimen APS avulla. Kuviosta 2 poiketen APRS voi olla myös eri verkossa kuin RNC, koska APRS on tyypillisesti operaattorikohtainen, eikä sinänsä ole mihinkään radioverkkoon sidottu. Tässä tapauksessa yhteys liityntäpisterekisteripalvelimeen APRS voidaan muodostaa myös muuta kautta kuin radioverkkokontrollerin RNC kautta.

Liityntäpistepalvelin APS osallistuu APRS:n ohjeiden mukaan paikallisesti AP:n liittämiseen kiinteän verkko-osan resursseihin, erityisesti radioverkkokontrolleriin RNC. Liityntäpistepalvelimen APS tärkeimpiä tehtäviä on valita liityntäpisteelle AP radioverkkokontrolleri RNC (RNC allocation) ja tarpeen mukaan konfiguroida valittu RNC tukemaan liityntäpistettä AP. Edelleen APS osallistuu tarpeen mukaan muiden tarvittavien verkkoresurssien varaamiseen liityntäpisteelle AP, kuten toiminnallisen yhteyden muodostamiseen runkoverkkoon CN. Liityntäpistepalvelimen APS hallintaan tyypillisesti kuuluu useita radioverkkokontrollereita RNC, on myös mahdollista, että APS on RNS-radioaliverkkokohtainen, eli liittyy tiettyyn radioverkkokontrolleriin RNC. APS voi tarjota myös tukea liityntäpisteiden AP liikkuvuudelle, eli se voi valita liityntäpisteelle AP vapaita resursseja omaavan radioverkkokontrollerin RNC operaattorin toiminta-alueen puitteissa. APS voi esimerkiksi valita lähimmän radioverkkokontrollerin palvelemaan liityntäpistettä AP. Lisäksi operaattorien välisillä roaming-sopimuksilla liityntäpisteille AP voidaan tarjota myös laajempi liikkuvuus toisten operaattoreiden toiminta-alueilla (verkkovierailu). Tästä on erityistä hyötyä liityntäpisteiden AP pienentyessä ja niiden siirrettävyyden helpottuessa. Liityntäpistepalvelin APS voi myös dynaamisesti hallita verkon eri osien kuormitusta muuttamalla liityntäpisteiden AP kytkentöjä eri verkkoelementteihin verkon kuormitustilanteen mukaan. Tällaisia verkkoelementtejä voivat olla esimerkiksi radioverkkokontrollerit RNC, synkronointipalvelimet ja muut verkon hajautetut yhteiset resurssit. Erillinen liityntäpistepalvelin APS ei ole välttämättä tarpeellinen, ainakin saman operaattorin alaisuuten kuuluvissa radioverkkokontrollereissa RNC APRS voi käsittää tarvittavan toiminnallisuuden RNC:n valitsemiseksi.

Liityntäpiste AP voi olla esimerkiksi yksittäisen henkilön tai yrityksen omistama tukiasema, jolloin IC-kortti ICC voi olla radioverkkokontrolleria RNC ja/tai runkoverkkoa CN hoitavan operaattorin tarjoama. Kuvioissa 2 ja 4 ha-

vainnollistetussa edullisessa suoritusmuodossa IC-kortin ICC käsittämät tiedot vaaditaan ehtona radioverkkokontrollerin RNC ja edelleen runkoverkon CN tarjoamien tiedonsiirtopalveluiden käytölle. Operaattori voi luovuttaa IC-kortin ICC valitsemilleen luotettaville tahoille, joilla on oikeus liittää liityntäpisteensä AP operaattorin kiinteään verkko-osaan ja hyödyntää verkko-osan resursseja. IC-kortti ICC voidaan autentikoida ja näin operaattori voi varmistua siitä, että ainoastaan sen kelpuuttama taho voi liittää liityntäpisteensä AP operaattorin verkkoelementteihin. Tämä mahdollistaa joustavan ja turvallisen tavan käyttää yksityisiä liityntäpisteitä ja tilapäisesti käyttää esimerkiksi vuokrattavia liityntäpisteitä IC-kortin käsittämien tietojen avulla. Maantieteellisesti kattava peitto edellyttää suurta määrää liityntäpisteitä, joiden ylläpitokustannukset voivat olla varsin korkeita. IC-kortin käyttäminen liityntäpisteissä AP tarjoaa operaattorille mahdollisuuden luovuttaa liityntäpisteiden AP hoidon jollekin valitsemallensa taholle tai ostaa liityntäpisteiden tarjoamat palvelut. Tämä vähentää huomattavasti tarvittavaa ylläpitotyötä ja operaattorit voivat keskittyä enemmän runkoverkon CN tarjoamiin palveluihin. Operaattori voi myös helpommin laajentua ostamalla liityntäpistepalvelut ulkopuolelta. Edelleen, vaikka liityntäpisteet olisivatkin saman operaattorin hallinnassa kuin kiinteä verkko-osa, keksinnön erään edullisen suoritusmuodon mukaisella IC-kortin käytöllä operaattori voi turvallisesti käyttää julkista verkkoa, kuten Internetiä, liityntäpisteen ja kiinteän verkko-osan välillä.

IC-kortille ICC tallennetaan pääsääntöisesti liityntäpisterekisteripalvelimen APRS omistajan, esimerkiksi runkoverkko-operaattorin, toimesta taulukossa 1 havainnollistettuja tietoja.

Yksilöllinen tunniste
APRS-osoite
Autentikointiin ja salaukseen liittyviä tietoja: - tarvittava yksi tai useampi salainen avain - tarvittavat algoritmit
Suoritettavia komentojonoja / sovelluksia
Muita tietoja: – liityntäpisteen konfigurointitietoja – järjestelmän toimintaan ja ylläpitoon liittyviä toiminnan aikana kerättäviä tietoja

Taulukko 1. IC-kortin käsittämiä tietoja

ICC käsittää yksilöllisen tunnisteen (Specific Identity), jonka perusteella IC-kortin ICC tiedot voidaan erottaa muista liityntäpisterekisteripalvelimen APRS käsittämistä tiedoista. Jotta yhteys voidaan muodostaa liityntäpisterekisteripalvelimeen APRS, IC-kortille tallennetaan APRS:n verkko-osoite (APRS-osoite). APRS-osoite voi olla esimerkiksi IP-osoite tai URL-tunniste (Uniform Resource Locator). ICC käsittää tietoja, kuten yhden tai useampia salaisia avaimia ja tarvittavia algoritmeja, kortin autentikoimiseksi ja liityntäpisteen ja kiinteän verkko-osan elementin, tyypillisesti radioverkkokontrollerin RNC, välisen yhteyden salaamiseksi tarvittaessa. Edellä kuvatut tiedot ovat olennaisia, jotta operaattori voi sallia IC-kortin käsittävän liityntäpisteen AP pysyvämmän liittämisen verkkoonsa.

Koska ICC tyypillisesti käsittää suorittimen CPU, IC-kortin ICC tietoihin voidaan myös tallentaa suoritettavia käskysekvenssejä eli sovelluksia. Näiden sovellusten avulla voidaan toteuttaa järjestelmän ja erityisesti liityntäpisteen AP käyttöön, ylläpitoon, valvontaan ja poikkeustilanteiden käsittelyyn liittyviä toimintoja. Salausavaimen/avaimien käsittely IC-kortilla ICC on yksi tyypillinen esimerkki kortille tallennettavasta sovelluksesta. Suoritettavat ohjelmat voidaan tallentaa IC-kortille ICC joko etukäteen osana kortin ohjelmointia ennen käyttöönottoa tai ladata dynaamisesti tietoliikenneverkkoa hyväksi käyttäen.

IC-kortin ICC omistava operaattori voi esimerkiksi tallentaa omia sovelluksiaan, joiden avulla se voi saada tietoa liityntäpisteen AP käytöstä. IC-kortin ICC käsittämä sovellus voi tietyin väliajoin tai operaattorin välittämän pyynnön perusteella kerätä tietoa esimerkiksi käyttäjien määrästä ja välittää tämän tiedon liityntäpisteen AP ja kiinteän verkko-osan välistä yhteyttä hyödyntäen liityntäpistepalvelimelle APS. IC-kortin ICC käsittämiä sovelluksia voidaan ohjata edullisesti liityntäpistepalvelimella APS olevalla kontrolliohjelmistolla, jonka avulla IC-kortin sovelluksen välittämää tietoa voidaan myös edelleen hyödyntää.

IC-kortti ICC voi käsittää myös muita tietoja, kuten liityntäpisteen AP konfigurointitietoja. Konfigurointitiedot voivat käsittää esimerkiksi tietoja radiorajapintaan liittyvistä asetuksista, kuten sallitusta taajuusalueesta, tai tietoja liityntäpisteen AP ja kiinteän verkko-osan välisistä asetuksista. Esimerkiksi, jos liityntäpisteen AP ja kiinteän verkko-osan välillä käytetään Internetiä, tietoja käytettävästä yhdyskäytävästä (gateway), nimipalvelimesta tai välimuistipalvelimesta (proxy server) voi olla tallennettuna IC-kortille ICC. Edelleen muut tie-

dot voivat käsittää erilaisia liityntäpisteen käyttöön ja ylläpitoon liittyviä tietoja, esimerkiksi käytönaikaista tietoja liikenteestä, käyttäjistä, laskutuksesta sekä tietoa virhe- ja poikkeustilanteista.

Kuvio 3 esittää sinänsä jo tunnetun IC-kortin ICC sisäistä rakennetta pelkistettynä lohkokaaviona. IC-kortti ICC on tyypillisesti luottokortin kokoinen muovinen kortti, johon on asetettu mikropiiri. IC-kortin ICC pinnassa on sähköiset kontaktit, joiden välityksellä voidaan välittää käyttöjännitteet kortille sekä siirtää ohjaus- ja datasignaaleja lukulaitteen, kuten liityntäpisteen AP korttivälineiden ICCM ja IC-kortin ICC väyläsovittimen DATA I/O välillä. Tiedonsiirto IC-kortin ICC ja liityntäpisteen korttivälineiden ICCM välillä tapahtuu siis väyläsovittimen DATA I/O kautta.

Suoritin CPU (Central Processing Unit) ohjaa IC-kortin ICC toimintaa muistiin ICCMEM, tyypillisesti ohjelmamuistiin ROM (Read Only Memory), tallennetun ohjelmakoodin perusteella. Tietomuistiin EEPROM (Electrically Erasable Programmable Read-Only Memory) voidaan tallettaa erilaista käyttäjäkohtaista tietoa, joka säilyy muistissa olennaisesti pysyvästi. Edellä kuvattuja tietoja liittyen IC-kortin käyttöön liityntäpisteessä AP voidaan edullisesti tallentaa tietomuistiin EEPROM. IC-kortin ICC käsittämät tiedot on järjestetty eri hakemistoihin, joihin on erilaiset käyttöoikeudet kortilla ja ulkopuolisilla laitteilla. Käyttömuistia RAM (Random Access Memory) voidaan käyttää väliaikaisena tiedon talletuspaikkana. IC-kortilla ICC on käyttöturvallisuuden varmentamiseksi turvatoiminto SEC, joka hoitaa mm. PIN-tunnuksen tarkistamisen. Kuten jo todettiin, liityntäpiste AP käsittää korttivälineet ICCM IC-kortin ICC käyttämiseksi, lähinnä lukuvälineet sähköisten kontaktien lukemiseksi ja edullisesti myös kirjoitusvälineet IC-kortin ICC muistiin kirjoittamiseksi ohjausyksikön CONTROL antamien signaalien mukaisesti.

Riippuen halutusta toteutuksesta, IC-kortti ICC voi käsittää moniakin itsenäisesti toimivia sovelluksia, jotka voivat antaa pyyntöjä liityntäpisteen AP ohjausyksiköllle CONTROL. Toisena ääripäänä ohjausyksikkö CONTROL voidaan järjestää ohjaamaan täysin orjana (slave) toimivaa IC-korttia ICC, jolloin IC-kortti ICC toimii lähinnä tietojen säilytyspaikkana. Edullisessa suoritusmuodossa ohjausyksikkö CONTROL käsittää varsinaisen toiminnallisuuden IC-kortin ICC tietojen (myös mahdollisten sovellusten) hyödyntämiseksi ja edullisesti myös tietojen tallentamiseksi IC-kortille ICC. Liityntäpisteen AP ja IC-kortin ICC välillä voidaan käyttää samoja fyysisiä ja loogisia määrityksiä kuin UMTS:n USIM-sovelluksen käsittävän UICC-kortin (UMTS IC Card) ja UMTS-

päätelaitteen välillä, joiden tarkemman kuvauksen osalta viitataan 3GPP:n spesifikaatioon TS 31.101 "UICC-Terminal Interface; Physical and Logical Characteristics".

IC-kortti ICC voi käsittää myös muihin tarkoituksiin tallennettuja tietoja, eli IC-kortti voi olla ns. monisovelluskortti (Multi-application Card). IC-kortille ICC voi olla esimerkiksi tallennettu usean eri operaattorin tietoja, jolloin liityntäpisteestä AP voidaan muodostaa yhdellä kortilla yhteyksiä eri operaattoreiden radioverkkokontrollereihin RNC ja runkoverkkoihin CN.

Seuraavassa kuvataan esimerkinomaisesti IC-kortin ICC aktivointia: IC-kortti ICC asetetaan liityntäpisteeseen AP, jonka korttivälineet ICCM kytkevät siihen käyttöjännitteen. ICC välittää liityntäpisteelle AP tietoja ominaisuuksistaan, esimerkiksi sen tukemat protokollat ja valmistajatiedot. Jos kortti ICC on hyväksyttävä, liityntäpiste AP tarkastaa PIN-tunnisteen käyttäjältä tai useissa tapauksissa käyttöönottajalta käyttöliittymän, esimerkiksi näppäimistön, mikrofonin tai paineltavan näyttöruudun avulla. Turvalogiikka SEC tarkistaa, onko syötetty PIN-tunniste oikea. Jos tunniste on oikea, IC-kortti ICC on käytettävissä. Näin voidaan varmistaa, että vain PIN-tunnisteen tunteva käyttäjä voi hyödyntää IC-korttia ICC. Käyttäjän tunnistaminen voidaan suorittaa millä tahansa muullakin tavalla, esimerkiksi käyttämällä sormenjäljen tunnistusta (Fingerprint Recognition). Jos käyttäjän tunnistaminen onnistuu, kortti on valmis käytettäväksi.

Viitaten kuvioon 4 selostetaan keksinnön kannalta olennaiset asiat huomioiden tarkemmin tukiasemana toimivan liityntäpisteen AP liittämistä kiinteään verkko-osaan IC-kortin käsittämien tietojen avulla. Kun liityntäpisteessä AP aktivoidaan 400 (ICC activation) IC-kortti ICC, AP voi alkaa aktiivisesti hakemaan kiinteän verkko-osan elementtiä, johon se voisi liittyä. Jos käyttäjällä on oikeus käyttää IC-korttia ICC (esim. PIN-tunniste on oikea) ja kortin aktivoiminen onnistuu, liityntäpiste AP pyytää 401 (request data) IC-kortin ICC hakemistoista ainakin liityntäpisterekisteripalvelimen APRS osoitetiedon ja yksilöllisen tunnisteen. APRS:n osoite voi olla esimerkiksi IP-osoite. IC-kortilta ICC välitetään ainakin yksilöllisen tunnisteen ja APRS:n osoitetiedon käsittävä vastine 402 (reply data), jonka perusteella AP voi lähettää 403 yksilöllisen tunnisteen käsittävän yhteyspyynnön (connection request) liityntäpisterekisteripalvelimelle APRS.

Yhteys liityntäpisteen AP ja liityntäpisterekisterin APRS välille voidaan muodostaa sinänsä jo tunnettuja ratkaisuja hyödyntämällä. Esimerkiksi,

jos yhteys on Internetin kautta, voidaan käyttää VPN-tekniikkaa. IC-kortille ICC voi olla tallennettuna liityntäpisterekisteripalvelimeen APRS kuuluva VPN-numero, jonka perusteella AP voi kapseloida paketit niin, että ainoastaan APRS voi purkaa kapseloinnin. Käytössä voi olla myös erilliset VPN-toiminnallisuuden käsittävät palvelimet.

Saadessaan yhteyspyynnön 403, APRS edullisesti tarkastaa, onko välitetyn yksilöllisen tunnisteen mukaisella IC-kortilla ICC oikeus käyttää kiinteän verkko-osan resursseja. Oikeuksien tarkistus käsittää edullisesti tietojen tarkastuksen tietokannasta yksilöllisen tunnisteen perusteella ja myös IC-kortin autentikoimisen sen varmistamiseksi, että pyyntö todella tulee IC-kortilta ICC. Jos IC-kortin ICC tiedot löytyvät liityntäpisterekisteripalvelimen APRS tietokannasta, APRS voi autentikoida 404 (ICC authentication) IC-kortin ICC toisaalta IC-kortilta välitettyjen tietojen ja toisaalta APRS:n tietokannan käsittämien tietojen perusteella. Autentikoinnin erästä mahdollista toteutusta kuvataan tarkemmin myöhemmin. On myös mahdollista, että liityntäpisteellä AP on oma yksilöllinen tunnisteensa, jonka APRS haluaa tarkastaa ennen kuin se antaa liityntäpisteelle AP oikeuden yhteyden muodostamiseen kiinteään verkko-osaan. Tällöin AP voi APRS:n pyynnöstä välittää tunnisteensa. APRS voi käsittää listan hyväksytyistä ja/tai kielletyistä laitteista, jolloin se voi estää esimerkiksi ilman tyyppihyväksyntää olevien liityntäpisteiden pääsyn kiinteän verkko-osan resursseihin.

Jos ICC saadaan autentikoitua hyväksyttävästi ja APRS voi oikeuttaa liityntäpisteen saamaan yhteyden kiinteään verkko-osaan, kiinteästä verkko-osasta voidaan varata tarvittavat resurssit liityntäpisteelle AP. APRS valitsee liityntäpisteelle AP liityntäpistepalvelimen APS. APRS voi valita käytettävän liityntäpistepalvelimen APS kiinteästi annetun valmiin kytkentätaulukon perusteella tai optimoimalla haluttuja parametreja. Optimoitavia parametrejä voivat olla verkkoelementtien kuormitus ja kapasiteetti, siirtoteiden kuormitus ja kapasiteetti, siirtoviiveiden minimointi, kustannukset. APRS voi hakea edullista reittiä käyttämällä esimerkiksi Internetin solmujen reititystietoja hyväkseen. APRS voi myös pyrkiä minimoimaan viivettä lähettämällä kiertokyselyn (polling) esimerkiksi käyttämällä IP-protokollan mukaista ping-komentoa ehdolla olevien verkkoresurssien ja liityntäpisteen AP välillä. Jos siirtotienä on vuokrattu verkko, voidaan resurssin valinta suorittaa myös minimoimalla siirtokustannukset.

APRS välittää valtuutuksen 405 (authorization) valitsemalleen liityntäpistepalvelimelle APS ja vahvistuksen 406 (confirmation) yhteyspyynnön onnistumisesta liityntäpisteelle AP. Valtuutus 405 käsittää tiedon, edullisesti yksilöllisen tunnisteen, IC-kortista ICC, jolle resursseja voidaan varata. Valtuutus 405 voi käsittää myös salauksen toteuttamiseen tarvittavia tietoja, kuten lasketun salausavaimen. Tästä syystä liityntäpisterekisteripalvelimen APRS ja liityntäpistepalvelimen APS välinen yhteys on edullisesti suojattu. APS päivittää valtuutuksen 405 perusteella tietonsa uudella tuettavalla liityntäpisteellä AP. Vahvistus 406 käsittää myös liityntäpistepalvelimen APS osoitetiedon.

AP voi saadessaan vahvistuksen 406 lähettää liityntäpistepalvelimelle APS pyynnön liityntäpisteen AP liittämisestä kiinteään verkko-osaan, edullisesti 407 (RNC request) radioverkkokontrolleriin RNC. APS varaa liityntäpisteelle AP yhteyden tarjoavan radioverkkokontrollerin RNC 408 (RNC selection) saadessaan pyynnön 407. Tällöin radioverkkokontrolleriin RNC voidaan tallentaa tietoja uudesta liityntäpisteestä AP, edullisesti ainakin AP:n identifioiva tunniste ja AP:n fyysinen osoite. Käytettävä salausavain välitetään myös edullisesti RNC:lle. Kun RNC on valittu, APS välittää tästä vahvistuksen 409 (RNC confirmation) liityntäpisteelle AP. Vahvistus 409 käsittää myös valitun radioverkkokontrollerin RNC osoitetiedon. Liityntäpisteen AP asetukset muutetaan vahvistuksen 409 mukaisesti ja AP:n ja RNC:n välille voidaan tämän jälkeen muodostaa yhteys 410 (connection setup). Liityntäpisteen AP liittäminen radioverkkokontrolleriin RNC voidaan suorittaa lub-rajapintamääritysten mukaisella NBAP-signaloinnilla (NodeB Application Part), jolloin radioverkkokontrollerista RNC voidaan välittää tarvittavia konfigurointitietoja ja ohjauskomentoja liityntäpisteelle AP. Osa tässä vaiheessa tarvittavista konfigurointitiedoista, kuten tieto sallitusta taajuusalueesta voi olla myös tallennettuna IC-kortille ICC, jolloin AP:n asetukset muutetaan tallennettujen konfigurointitietojen mukaisiksi. RNC:n resursseista varataan osa liityntäpisteelle AP ja RNC:n solutiedot päivitetään yhdellä tai useammalla liityntäpisteen AP solulla. Liityntäpisteessä AP voidaan edullisesti salata lähetettävä informaatio ja avata RNC:n salaama informaatio käyttämällä IC-kortilla ICC käytettyä salausavainta, jolloin tiedonsiirto on turvallista mahdollisesti julkisen verkon kautta olevan lub-rajapinnan yli. Vastaavasti myös RNC:ssä otetaan edullisesti käyttöön APS:n välittämä salausavain. Eräs tapa on myös käyttää VPN-tekniikkaa myös liityntäpisteen AP ja radioverkkokontrollerin RNC välisen yhteyden suojaamiseen. Liityntäpiste AP voidaan liittää myös tarvittaviin runko-

verkon CN resursseihin operointisolmussa SGSN ja/tai matkaviestinkeskuksessa 3GMSC/VLR. Liityntäpisteen AP solutunnus (cell-id) välitetään edullisesti runkoverkkoon CN ainakin laskutuksen järjestämiseksi. Solutunnus voidaan laskutuksen hoitavassa elementissä rinnastaa palvelualueeseen (service area), jonka perusteella liityntäpisteen AP alueella olevia käyttäjiä voidaan laskuttaa.

Kun toiminnallinen yhteys tarvittaviin resursseihin on muodostettu, liityntäpisteen AP kautta voidaan edullisen suoritusmuodon mukaisesti hyödyntää radioverkkokontrolleria RNC ja edelleen siihen liittyvää runkoverkkoa CN. AP voi alkaa tarjoamaan palveluitaan peittoalueensa päätelaitteille UE aloittamalla solussaan broadcast-lähetykset BCH-kanavassa (Broadcast Channel) (BCH broadcast) ja RACH-kanavan (Random Access Channel) monitoroinnin. Jos keksintöä sovelletaan UMTS-järjestelmän FDD-moodissa, liityntäpiste AP voidaan makrodiversiteetin toteuttamiseksi eri solujen välillä liittää radioverkkokontrollerin RNC lisäksi toiminnalliseen yhteyteen myös yhteen tai useampaan liityntäpisteeseen. Liityntäpisteiden välinen yhteys tyypillisesti hoidetaan radioverkkokontrollerin RNC kautta.

IC-kortti ICC voidaan autentikoida monella eri tavoin. Kuviossa 5 on havainnollistettu erästä autentikointimenetelmää, jonka yhteydessä lasketaan myös käytettävät salausavaimet. Autentikointi voidaan aloittaa 500 esimerkiksi liityntäpisteen AP välittämän pyynnön perusteella. Liityntäpisterekisteripalvelimessa APRS valitaan 501 IC-korttia ICC varten satunnaislukuparametri ja lasketaan ICC-kortin yksilöllisen tunnisteen mukaisen salaisen avaimen ja satunnaisluvun perusteella autentikoinnin tarkastusparametri eli autentikointivaste ja salausavain (Cipher Key). Satunnaislukuparametri ja mahdollinen vastapuolen tunnistukseen käytettävä varmistustunnus välitetään 502 liityntäpisteelle AP, jonka kontrollivälineet CONTROL on järjestetty välittämään vastaanotetut tiedot käsittävä pyyntö autentikoinnista ja salausavaimen laskemisesta IC-kortille ICC. Jos varmistustunnus on hyväksyttävä, ICC laskee 503 satunnaisluvun ja salaisen avaimen avulla salaus-/autentikointialgoritmeja käyttäen autentikointivasteen ja salausavaimen. ICC välittää 504 laskemansa autentikointivasteen AP:lle, jonka kontrollivälineet CONTROL edelleen välittävät sen verkkoon APRS:lle. APRS vertaa 505 laskemaansa autentikointivastetta IC-kortilla laskettuun autentikointivasteeseen. Jos verkossa laskettu autentikointivaste ja IC-kortilla ICC laskettu autentikointivaste ovat samoja, autentikointi on hyväksyttävä 507 ja ollaan varmistuttu siitä, että kyseessä on autenttisesti APRS:n tie-

tojen mukainen IC-kortti ICC. Jos autentikointivasteet eivät ole samoja, autentikointi ei ole hyväksyttävä 506. On myös mahdollista, että APRS ja IC-kortti ICC välittävät laskemansa autentikointivasteet liityntäpistepalvelimelle APS, joka suorittaa vertauksen. Jos autentikointi on onnistunut hyväksyttävästi 507, salausavaimet voidaan välittää salauksen suorittaville elementeille, kuten liityntäpisteen AP lähetinvastaanotinvälineille TXRX ja radioverkkokontrollerille RNC.

Kuten jo aiemmin on mainittu, IC-korttia ICC voidaan hyödyntää liityntäpisteen AP käyttöön, ylläpitoon tai seurantaan liittyvissä tehtävissä. Kun liityntäpiste AP on liitetty kiinteään verkko-osaan, radioverkkokontrollerlin RNC ja tyypillisesti edelleen runkoverkkoon CN, toiminnallisen yhteyden säilyttämiseksi IC-kortti ICC voidaan autentikoida tietyin väliajoin ja myös käytettävä salausavain voidaan vaihtaa riittävän turvallisuuden varmistamiseksi. Toiminnallinen yhteys voidaan purkaa liityntäpisteen AP lähettämän pyynnön perusteella tai IC-kortin omistajan, esimerkiksi ydinverkkoa CN hallitsevan operaattorin niin halutessa. Kun liityntäpisteen AP ja kiinteän verkko-osan välinen toiminnallinen yhteys puretaan, voidaan liityntäpisteen AP tiedot poistaa radioverkkokontrollerista RNC ja liityntäpistepalvelimesta APS.

On huomioitava, että kuvion 4 yhteydessä kuvattu liityntäpisteen AP liittäminen kiinteän verkko-osan resursseihin on vain yksi mahdollinen toteutusesimerkki ja itse signalointisekvenssi voidaan toteuttaa usealla eri tavalla, kuitenkin siten, että edullisessa suoritusmuodossa liityntäpiste AP aloittaa signaloinnin käyttäen IC-kortille ICC tallennettua liityntäpisterekisteripalvelimen APRS osoitetta. Ilman IC-korttia ICC liityntäpiste AP voi toimia kuten liityntäpisteet AP tälläkin hetkellä toimivat, eli odottavat ohjausta kiinteästä verkko-osasta, eivätkä lähde aktiivisesti kytkeytymään verkkoon. Edelleen, IC-kortti ICC voidaan aiemmasta kuvauksesta poiketen asettaa liityntäpisteeseen AP toiminnallisessa yhteydessä olevaan laitteeseen, esimerkiksi reitittimeen. IC-korttia voidaan tämän laitteen kautta käyttää liityntäpisteen AP ja kiinteän verkon resurssien liittämisessä toiminnalliseen yhteyteen.

Edellä on kuvattu IC-kortin ICC hyödyntämistä liityntäpisteissä AP, jotka ovat UMTS-järjestelmän tukiasemia tai B-solmuja. Kuten on jo todettu, langattoman tietoliikennejärjestelmän liityntäpiste voi olla myös tukiasemia kontrolloiva radioverkkokontrolleri, jossa IC-korttia ICC voidaan keksinnön mukaisesti myös hyödyntää. IC-korttia ICC voidaan hyödyntää RNC:ssä RNC:n liittämiseen toiminnalliseen yhteyteen kiinteän verkko-osan resurssien, lähinnä

runkoverkon CN verkkoelementtien, kanssa. RNC käsittää tällöin korttivälineet IC-kortin ICC käyttämiseksi, kontrollivälineet ja lähetinvastaanottimen toiminnallisen yhteyden muodostamiseksi tarvittaviin kiinteän verkon resursseihin IC-kortille tallennettujen tietojen perusteella. IC-kortille ICC voidaan tallentaa taulukossa 1 esitettyjä tietoja, edullisesti yksilöivä tunniste, APRS:n osoite, autentikaation ja salaukseen tarvittavia tietoja. Jos käytetään palvelimia APS ja APRS, kuviosta 2 poiketen, liityntäpisterekisteripalvelin APRS ja liityntäpistepalvelin APS voivat sijaita tällöin runkoverkossa CN. Kuten jo aiemmin on todettu, APRS käsittää tietoja IC-kortin ICC oikeuksien tarkistamiseksi edullisesti yksilöllisen tunnisteen ja autentikoinnin avulla. APS:n tehtävänä on ohjata yhtä tai useampaa runkoverkon CN elementtiä, kuten matkaviestinkeskusta 3GMSC/VLR tai operointisolmua SGSN, liittämään resurssejaan RNC:n kanssa toiminnalliseen yhteyteen. Liityntäpisteen (RNC) liittäminen voidaan suorittaa kuvion 4 yhteydessä esitetyllä tavalla sillä poikkeuksella, että liittäminen tapahtuu runkoverkkoon CN. Tällöin APRS:n antaessa APS:lle käskyn RNC:n liittämisestä ja RNC:n mahdollisesti pyytäessä liittämistä APS:ltä, APS välittää tiedon liitettävästä RNC:stä runkoverkon CN elementille, eli operointisolmulle SGSN ja/tai matkaviestinkeskukselle 3GMSC/VLR. Pyyntö käsittää ainakin tiedon RNC:n fyysisestä osoitteesta. Runkoverkossa CN voidaan ottaa käyttöön RNC:n yksilöivä RNC-tunniste (RNC-id), jonka perusteella eri radioverkkokontrollerit erotetaan toisistaan. Ainakin yhden runkoverkon CN elementin ja RNC:n välille muodostetaan päästä-päähän (point-to-point) siirtoyhteys ja RNC sidotaan tiettyyn alueeseen runkoverkon CN elementissä, kuten sijaintialueeseen (location area matkaviestinkeskuksessa 3GMSC/VLR) tai reititysalueeseen (routing area operointisolmussa SGSN). Varsinaiset signalointi- ja datayhteydet luodaan runkoverkon CN ja RNC:n välille RANAP-signaloinnilla (Radio Access Network Application). Myös tarvittavia tietoja, kuten solutunnukset, RNC:n kuuluvista tukiasemista voidaan välittää runkoverkkoon CN. Näin RNC:n ja yhden tai useamman runkoverkon CN resurssien välille on muodostettu toiminnallinen yhteys, jolloin RNC:lle ja sen kontrolloimille tukiasemille voidaan luotettavasti tarjota runkoverkon CN palveluja. IC-kortin ICC autentikointi voidaan hoitaa esimerkiksi kuviossa 5 esitetyn tavan mukaisesti ja RNC:n ja kiinteän verkko-osan välinen liikenne voidaan salata lasketuja salausavaimia hyödyntäen.

IC-korttia ICC voidaan käyttää myös pelkästään langallisia yhteyksiä tarjoavien liityntäpisteiden, kuten laajakaistamodeemien (esim. ADSL,

Asynchronous Digital Subscriber Line), liittämisessä muihin tietoliikennejärjestelmän elementteihin, kuten puhelinkeskukseen. Tällöin IC-kortilla ICC olevia tietoja voidaan käyttää myös tarvittavien autentikointien ja salausten toteuttamisessa.

Alan ammattilaiselle on ilmeistä, että tekniikan kehittyessä keksinnön perusajatus voidaan toteuttaa monin eri tavoin julkisissa tai yksityisissä verkoissa. Keksintö ja sen suoritusmuodot eivät siten rajoitu yllä kuvattuihin esimerkkeihin vaan ne voivat vaihdella patenttivaatimusten puitteissa.

42

Patenttivaatimukset

1. Menetelmä liityntäpisteen liittämiseksi muihin verkkoelementteihin langattomassa tietoliikennejärjestelmässä, joka käsittää ainakin yhden liityntäpisteen ja ainakin yhden kiinteän verkko-osan, t u n n e t t u siitä, että:

tallennetaan IC-kortille tietoja ainakin yhden liityntäpisteen liittämiseksi toiminnalliseen yhteyteen kiinteän verkko-osan kanssa,

kytketään IC-kortti toiminnalliseen yhteyteen liityntäpisteen kanssa vasteena sille, että halutaan liittää liityntäpiste kiinteään verkko-osaan, ja

liitetään tarvittavia kiinteän verkko-osan resursseja liityntäpisteen kanssa toiminnalliseen yhteyteen mainittujen tallennettujen tietojen perusteella.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että

tarkastetaan kiinteässä verkko-osassa, onko IC-kortilla oikeus käyttää kiinteän verkko-osan resursseja, ja

liitetään tarvittavia kiinteän verkko-osan resursseja liityntäpisteen kanssa toiminnalliseen yhteyteen vasteena sille, että IC-kortilla on oikeus käyttää kiinteän verkko-osan resursseja.

3. Patenttivaatimuksen 2 mukainen menetelmä, t u n n e t t u siitä, että

mainitut tiedot käsittävät ainakin yhden kiinteän verkko-osan elementin osoitteen ja IC-kortille yksilöllisen tunnisteen,

kiinteän verkko-osan elementti käsittää myös tietoja IC-kortista yksilöllisen tunnisteen mukaisesti eroteltuna,

välitetään pyyntö liityntäpisteen liittämisestä tallennetun osoitteen perusteella kiinteän verkko-osan verkkoelementille, ja

tarkastetaan IC-kortin oikeudet tarkastamalla IC-kortin tiedot yksilöllisen tunnisteen perusteella ja autentikoimalla IC-kortti.

4. Patenttivaatimuksen 1, 2 tai 3 mukainen menetelmä, t u n n e t t u siitä, että

mainitut tiedot käsittävät IC-kortin autentikoimiseen tarvittavan ainakin yhden avaimen ja algoritmin,

välitetään ainakin yhden avaimen ja algoritmin avulla laskettu autentikointivaste kiinteään verkko-osaan,

autentikoidaan IC-kortti tarkastamalla välitetty autentikointivaste kiinteässä verkko-osassa, ja

liitetään liityntäpiste toiminnalliseen yhteyteen kiinteän verkko-osan resurssien kanssa vasteena sille, että autentikointivaste on hyväksyttävä.

5. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

mainitut tiedot käsittävät ainakin yhden avaimen ja algoritmin liityntäpisteen ja kiinteän verkko-osan välisen yhteyden salaamiseksi, ja

salataan liityntäpisteen ja kiinteän verkko-osan välinen liikenne ainakin yhtä avainta ja algoritmia hyödyntäen.

6. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

kiinteä verkko-osa käsittää ainakin yhden radioverkkokontrollerin, liityntäpistepalvelimen ja siihen toiminnallisessa yhteydessä olevan liityntäpisterekisteripalvelimen, johon on tallennettu IC-korttiin liittyviä tietoja, kuten IC-kortille yksilöllinen tunniste,

välitetään IC-kortin yksilöivä tunniste liityntäpisterekisteripalvelimelle,

tarkastetaan IC-kortin oikeus käyttää kiinteän verkko-osan resursseja,

valitaan liityntäpistepalvelin liityntäpisteelle vasteena sille, että IC-kortilla on oikeus käyttää kiinteän verkko-osan resursseja,

välitetään tieto valitusta liityntäpistepalvelimesta liityntäpisteelle ja tieto liitettävästä liityntäpisteestä liityntäpistepalvelimelle,

välitetään liityntäpisteestä liityntäpistepalvelimelle pyyntö radioverkkokontrollerin valitsemiseksi,

valitaan radioverkkokontrolleri liityntäpisteelle, ja

liitetään liityntäpiste radioverkkokontrollerin ja muiden mahdollisesti tarvittavien resurssien kanssa toiminnalliseen yhteyteen.

7. Patenttivaatimuksen 6 mukainen menetelmä, t u n n e t t u siitä, että

lasketaan IC-kortissa ja liityntäpisterekisteripalvelimessa ainakin yksi salausavain ja autentikointivaste,

välitetään IC-kortissa laskettu autentikointivaste liityntäpisterekisteripalvelimelle,

autentikoidaan IC-kortti tarkastamalla vastaako välitetty autentikointivaste liityntäpisterekisteripalvelimessa laskettua autentikointivastetta, ja

liitetään, vasteena hyväksyttävälle autentikoinnille, liityntäpiste radioverkkokontrollerin kanssa toiminnalliseen yhteyteen niin, että liityntäpisteen ja radioverkkokontrollerin välinen liikenne salataan laskettuja salausavaimia käyttäen.

8. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

IC-kortti käsittää turvatoiminnon IC-kortin käyttäjän tarkastamiseksi, ja

IC-kortille on tallennettu myös muuta dataa kuin mainittuja liityntäpisteiden käyttöön liittyviä tietoja, kuten UMTS-järjestelmän USIM-sovelluksessa tarvittavaa dataa.

9. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

liityntäpiste on UMTS-järjestelmän tukiasema ja kiinteä verkko-osa käsittää ainakin UMTS-järjestelmän radioverkkokontrollerin RNC.

10. Jonkin patenttivaatimuksen 1-8 mukainen menetelmä, t u n n e t t u siitä, että

liityntäpiste on UMTS-järjestelmän radioverkkokontrolleri RNC ja kiinteä verkko-osa käsittää yhden tai useampia UMTS-järjestelmän runkoverkon verkkoelementtejä.

11. Langaton tietoliikennejärjestelmä, joka käsittää ainakin yhden liityntäpisteen ja ainakin yhden kiinteän verkko-osan, t u n n e t t u siitä, että

liityntäpiste on järjestetty käyttämään IC-korttia, jolle on tallennettu tietoja ainakin yhden liityntäpisteen liittämiseksi toiminnalliseen yhteyteen kiinteän verkko-osan kanssa, ja

liityntäpiste ja kiinteä verkko-osa on järjestetty liittämään tarvittavia kiinteän verkko-osan resursseja liityntäpisteen kanssa toiminnalliseen yhteyteen mainittujen tallennettujen tietojen perusteella.

12. Patenttivaatimuksen 11 mukainen langaton tietoliikennejärjestelmä, t u n n e t t u siitä, että

kiinteä verkko-osa on järjestetty tarkastamaan, onko IC-kortilla oikeus käyttää kiinteän verkko-osan resursseja, ja

liityntäpiste ja kiinteä verkko-osa on järjestetty liittämään liityntäpiste ja tarvittavat kiinteän verkko-osan resurssit toiminnalliseen yhteyteen vasteena sille, että IC-kortilla on oikeus käyttää kiinteän verkko-osan resursseja.

13. Patenttivaatimuksen 12 mukainen langaton tietoliikennejärjestelmä, t u n n e t t u siitä, että

mainitut tiedot käsittävät ainakin yhden kiinteän verkko-osan elementin osoitteen ja IC-kortille yksilöllisen tunnisteen,

kiinteän verkko-osan elementti käsittää myös tietoja IC-kortista yksilöllisen tunnisteen mukaisesti eroteltuna,

liityntäpiste on järjestetty välittämään pyyntö liityntäpisteen liittämisestä tallennetun osoitteen perusteella kiinteän verkko-osan verkkoelementille, ja

kiinteän verkko-osan verkkoelementti on järjestetty tarkastamaan IC-kortin oikeudet tarkastamalla IC-kortin tiedot yksilöllisen tunnisteen perusteella ja autentikoimalla IC-kortti.

14. Jonkin patenttivaatimuksen 11-13 mukainen langaton tietoliikennejärjestelmä, t u n n e t t u siitä, että

kiinteä verkko-osa käsittää ainakin yhden radioverkkokontrollerin, liityntäpistepalvelimen ja siihen toiminnallisessa yhteydessä olevan liityntäpisterekisteripalvelimen, johon on tallennettu IC-korttiin liittyviä tietoja, kuten IC-kortille yksilöllinen tunniste,

liityntäpiste on järjestetty välittämään IC-kortin yksilöivä tunniste liityntäpisterekisteripalvelimelle,

liityntäpisterekisteripalvelin on järjestetty tarkastamaan IC-kortin oikeus käyttää kiinteän verkko-osan resursseja,

liityntäpisterekisteripalvelin on järjestetty valitsemaan liityntäpistepalvelin liityntäpisteelle vasteena sille, että IC-kortilla on oikeus käyttää kiinteän verkko-osan resursseja,

liityntäpisterekisteripalvelin on järjestetty välittämään tieto valitusta liityntäpistepalvelimesta liityntäpisteelle ja tieto liitettävästä liityntäpisteestä liityntäpistepalvelimelle,

liityntäpiste on järjestetty välittämään liityntäpistepalvelimelle pyyntö radioverkkokontrollerin valitsemiseksi,

liityntäpistepalvelin on järjestetty valitsemaan radioverkkokontrolleri liityntäpisteelle, ja

liityntäpiste ja kiinteä verkko-osa on järjestetty liittämään liityntäpiste radioverkkokontrollerin ja muiden mahdollisesti tarvittavien resurssien kanssa toiminnalliseen yhteyteen.

15. Patenttivaatimuksen 14 mukainen langaton tietoliikennejärjestelmä, t u n n e t t u siitä, että

IC-kortti ja liityntäpisterekisteripalvelin on järjestetty laskemaan ainakin yksi salausavain ja autentikointivaste,

liityntäpiste on järjestetty välittämään IC-kortissa laskettu autentikointivaste liityntäpisterekisteripalvelimelle,

liityntäpisterekisteripalvelin on järjestetty autentikoimaan IC-kortti tarkastamalla vastaako välitetty autentikointivaste liityntäpisterekisterissä laskettua autentikointivastetta, ja

liityntäpiste ja kiinteä verkko-osa on järjestetty liittämään, vasteena hyväksyttävälle autentikoinnille, liityntäpiste radioverkkokontrollerin kanssa toiminnalliseen yhteyteen niin, että liityntäpisteen ja radioverkkokontrollerin välinen liikenne salataan laskettuja salausavaimia käyttäen.

16. Langattoman tietoliikennejärjestelmän liityntäpiste, t u n n e t t u siitä, että

liityntäpiste käsittää korttivälineet IC-kortin syöttämiseksi liityntäpisteeseen ja IC-kortin käsittämien tietojen lukemiseksi, ja

liityntäpiste käsittää kontrollivälineet ja lähetinvastaanottimen toiminnallisen yhteyden muodostamiseksi tarvittaviin kiinteän verkko-osan resursseihin IC-kortille tallennettujen tietojen perusteella.

17. Patenttivaatimuksen 16 mukainen langattoman tietoliikennejärjestelmän liityntäpiste, t u n n e t t u siitä, että

mainitut tiedot käsittävät ainakin yhden kiinteän verkko-osan elementin osoitteen ja IC-kortille yksilöllisen tunnisteen,

kontrollivälineet on järjestetty lähettämään IC-kortin yksilöllisen tunnisteen käsittävä pyyntö liityntäpisteen liittämisestä tallennetun osoitteen perusteella kiinteän verkko-osan verkkoelementille, ja

kontrollivälineet on järjestetty muodostamaan toiminnallinen yhteys ainakin yhteen kiinteän verkko-osan verkkoelementtiin vasteena hyväksytylle pyynnölle liityntäpisteen liittämisestä.

18. Patenttivaatimuksen 16 tai 17 mukainen langattoman tietoliikennejärjestelmän liityntäpiste, t u n n e t t u siitä, että

kontrollivälineet on järjestetty välittämään pyyntö IC-kortille autentikointivasteen ja ainakin yhden salausavaimen laskemiseksi,

kontrollivälineet on järjestetty välittämään IC-kortilla laskettu autentikointivaste kiinteään verkko-osaan, ja

lähetinvastaanotinvälineet on järjestetty salaamaan kiinteälle verkko-osalle lähetettävä informaatio ja purkamaan kiinteältä verkko-osalta vastaanotettu informaatio IC-kortilla lasketun ainakin yhden salausavaimen avulla.

19. Jonkin patenttivaatimuksen 16-18 mukainen liityntäpiste, t u n n e t t u siitä, että

liityntäpiste on langattoman tietoliikennejärjestelmän tukiasema.

20. Jonkin patenttivaatimuksen 16-18 mukainen liityntäpiste, t u n n e t t u siitä, että

liityntäpiste on langattoman tietoliikennejärjestelmän yhtä tai useampaa tukiasemaa kontrolloiva radioverkkokontrolleri ja kiinteä verkko-osa käsittää yhden tai useampia langattomia tietoliikennejärjestelmän runkoverkon verkkoelementtejä.

L3

(57) Tiivistelmä
Menetelmä liityntäpisteen liittämiseksi muihin verkkoelementteihin langattomassa tietoliikennejärjestelmässä, joka käsittää ainakin yhden langattomia yhteyksiä tarjoavan liityntäpisteen ja ainakin yhden kiinteän verkko-osan. IC-kortille tallennetaan tietoja ainakin yhden liityntäpisteen liittämiseksi toiminnalliseen yhteyteen kiinteän verkko-osan kanssa. IC-kortti kytketään toiminnalliseen yhteyteen liityntäpisteen kanssa, jos halutaan liittää liityntäpiste kiinteään verkko-osaan. Tarvittavia kiinteän verkko-osan resursseja liitetään liityntäpisteen kanssa toiminnalliseen yhteyteen mainittujen tallennettujen tietojen perusteella. Kiinteässä verkko-osassa voidaan myös liittämisen ehtona tarkastaa, onko IC-kortilla oikeus käyttää kiinteän verkko-osan resursseja.
(Kuvio 4)

24

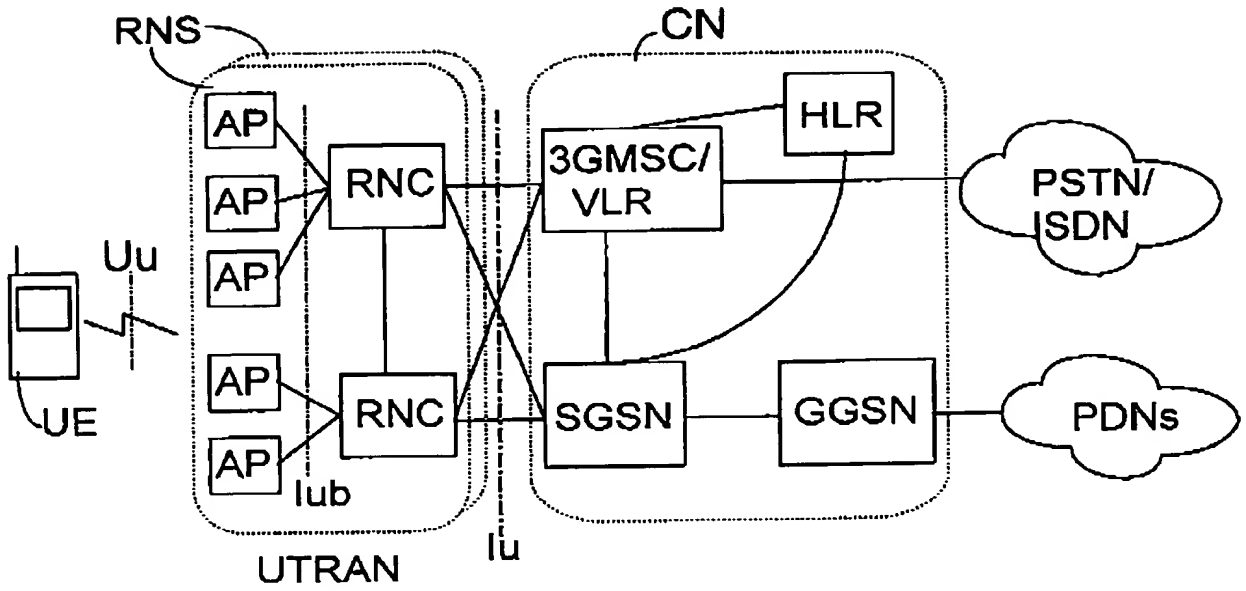
RNS
CN
AP
AP
AP
AP
AP
RNC
RNC
3GMSC/
VLR
HLR
PSTN/
ISDN
Uu
UE
SGSN
GGSN
PDNs
Iub
Iu
UTRAN

Fig. 1

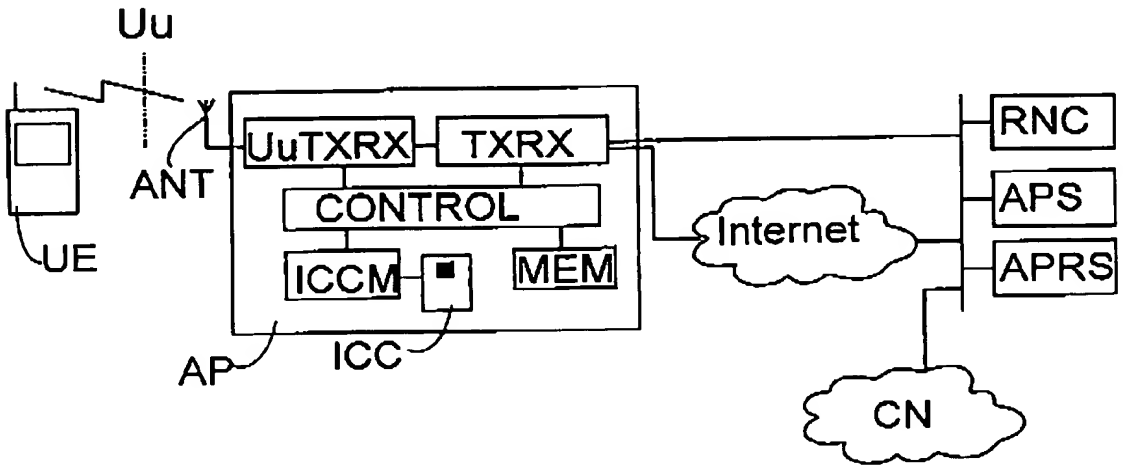
Uu
ANT
UE
UuTXRX
TXRX
CONTROL
ICCM
MEM
AP
ICC
Internet
RNC
APS
APRS
CN

Fig. 2

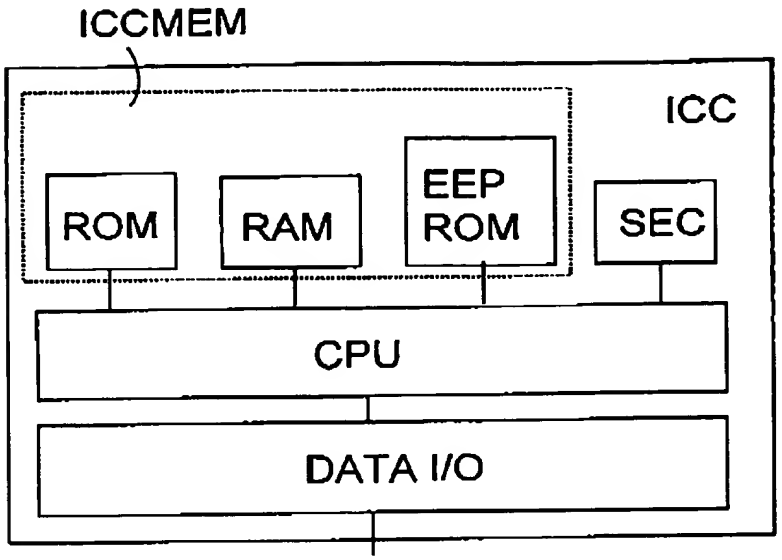
ICCMEM
ICC
ROM
RAM
EEP ROM
SEC
CPU
DATA I/O

Fig. 3

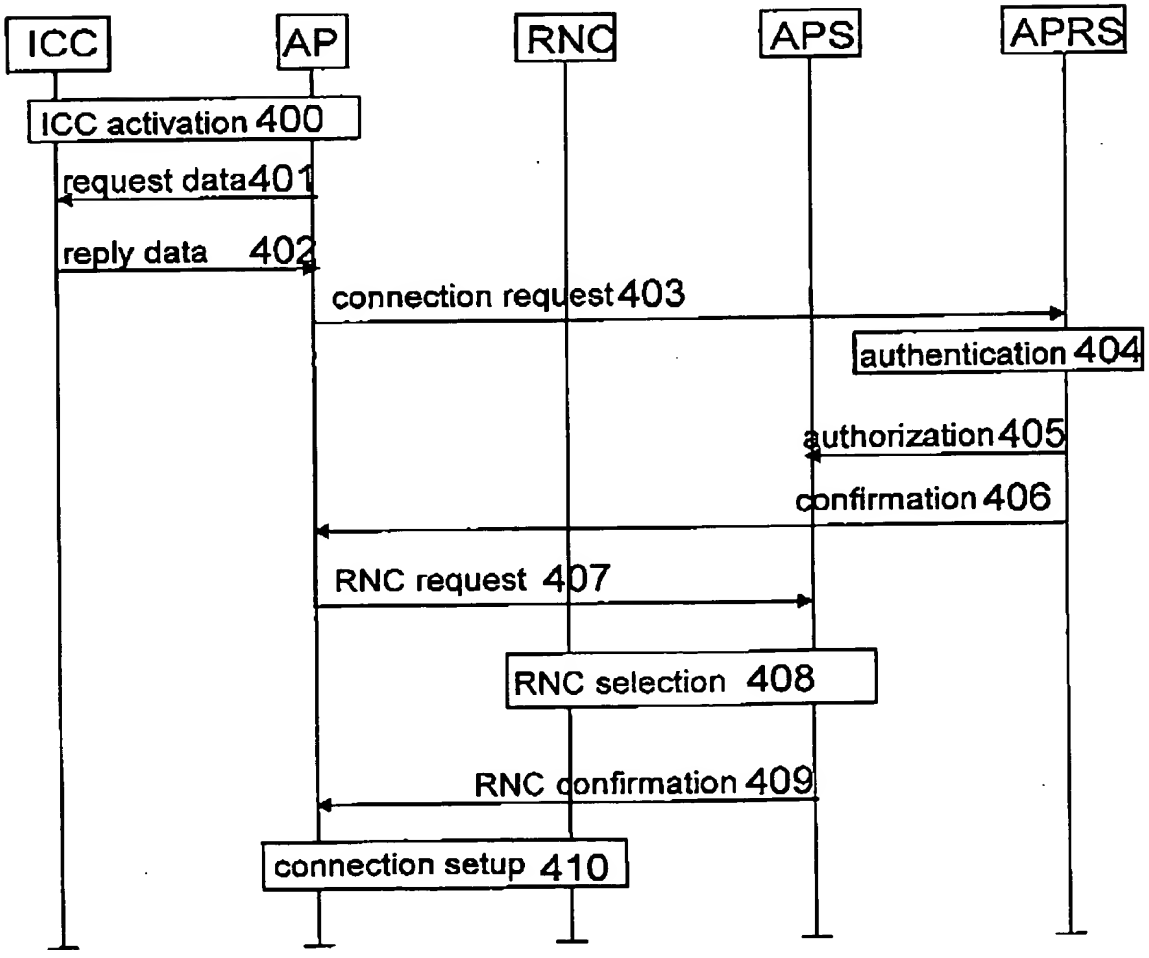
ICC
AP
RNC
APS
APRS
ICC activation 400
request data 401
reply data 402
connection request 403
authentication 404
authorization 405
confirmation 406
RNC request 407
RNC selection 408
RNC confirmation 409
connection setup 410

Fig. 4

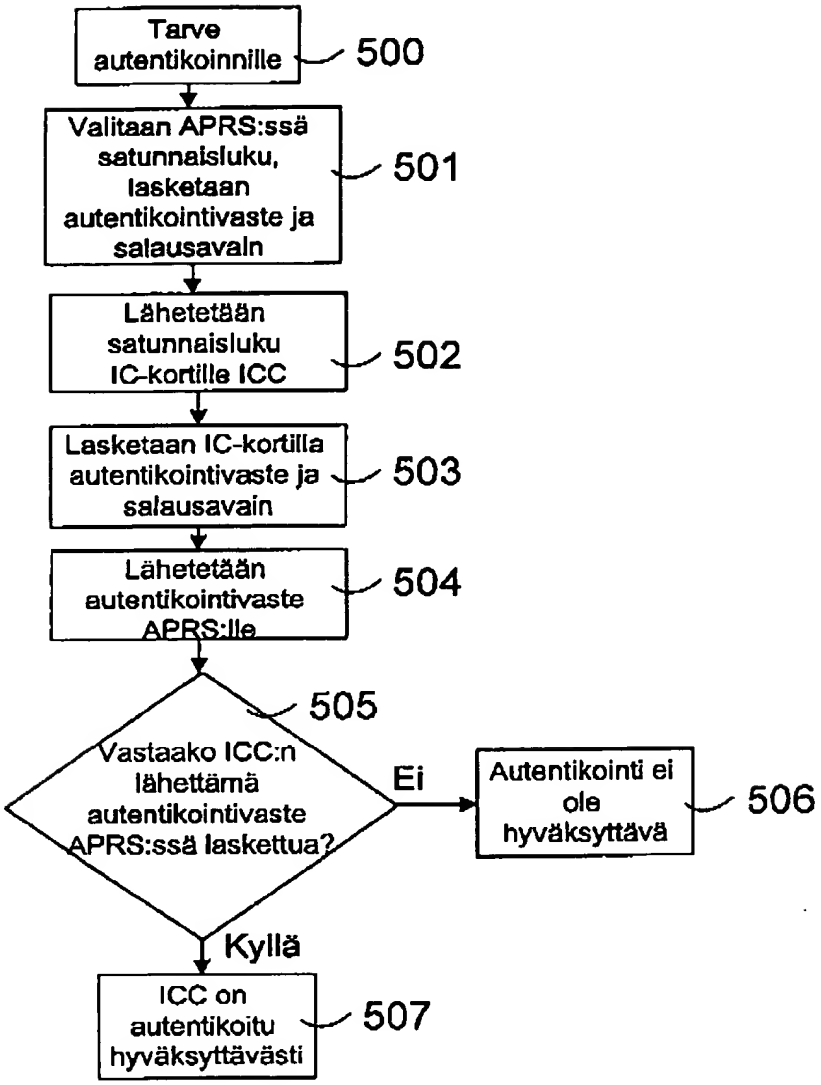
Tarve autentikoinnille
500
Valitaan APRS:ssä satunnaisluku, lasketaan autentikointivaste ja salausavain
501
Lähetetään satunnaisluku IC-kortille ICC
502
Lasketaan IC-kortilla autentikointivaste ja salausavain
503
Lähetetään autentikointivaste APRS:lle
504
505
Vastaako ICC:n lähettämä autentikointivaste APRS:ssä laskettua?
Ei
Autentikointi ei ole hyväksyttävä
506
Kyllä
ICC on autentikoitu hyväksyttävästi
507

Fig. 5